Google scholar dividing encryption sequence with mixing dum Search | Advanced Scholar Search

Scholar Articles and patents ▼ anytime ▼ include citations ▼ Create email alert

Results **1 - 10** of about **742**. **(0.03 sec)**

Encryption processing apparatus, **encryption processing** method, and computer program
R Oshi... - US Patent App. 10/749,412, 2004 - Google Patents
... By **dividing** an original **encryption processing sequence** into a ... 12 (START) > f **DIVIDE ENCRYPTION PROCESSING SEQUENCE** TO A PLURALITY OF GROUPS > f ... PREDETERMINED CONDITIONS IN ORDER TO SET **MIXING PROCESSING SEQUENCE** > r SEQUENTIALLY ...
All 2 versions

Encryption protection method
V Dupaquis... - US Patent App. 11/358,979, 2006 - Google Patents
... 3) a nonlinear substitution transformation taking the 48-bit key-mixed output, **dividing** it into ... For example, Rijndael, adopted as the Advanced **Encryption** Standard (AES), and published in ... their actions, but the inside masking **sequence** differs from the global masking **sequence**. ...
All 3 versions

High-speed VLSI architectures for the AES algorithm [PDF] from ieg-batpoon.com
X Zhang ... - Very Large Scale Integration (VLSI) ..., 2004 - ieeexplore.ieee.org
... clock period is determined by the indivisible component with the longest delay, **dividing** the rest ... to be divided into more substages to achieve the same speed as the **encryption** round unit ... The invMixColumns archi- tecture is **divide** into two parts according to the dashed line in Fig ...
Cited by 116 - Related articles - All 8 versions

Parallel **mixing** [PDF] from psu.edu
P Golle, A Juels - Proceedings of the 11th ACM conference on ..., 2004 - portal.acm.org
... A naive approach would be to **divide** the set of n inputs into k batches each ... ideal source of randomness, the adversary has no control over the **initial** division of slots into ... our parallel re-**encryption** mixnet protocol compares with a sequential synchronous re- **encryption** mixnet ...
Cited by 95 - Related articles - All 35 versions

Cryptographic defense against traffic analysis
C Rackoff ... - Proceedings of the twenty-fifth annual ACM ..., 1993 - portal.acm.org
... the network, is being sent. On the other hand, this "trivial" solution may require each party to **divide** the maximum rate at which it sends "legitimate" messages (and the network to **divide** the number of ... sociated with a particular public **encryption** key, ... the alo of the **mix** node. ...
Cited by 97 - Related articles - BL Direct - All 2 versions

INFORMATION **PROCESSING** DEVICE, DISC, INFORMATION **PROCESSING** METHOD, AND PROGRAM
R Nishida - US Patent App. 20/060/154,314, 2008 - freepatentsonline.com
... 20060209640, Method for **dividing** user storage space of an optical disc, optical disc ... ID), and execute a **process**, such as authentication **process** or cryptography **process**, in accordance ... 12 is a flowchart that illustrates a **processing sequence** between the application and the BCA ...
Cached

[PDF] ISDN-mixes: Untraceable communication with very small bandwidth overhead [PDF] from psu.edu
A Pfitzmann, B Pfitzmann ... - Proc. GI/ITG-Conference" ..., 1991 - Citeseer
... This can be provided together with end-to-end **encryption**: The unencrypted message inside N must fulfil a redundancy criterion; and B decrypts each ... The solution to the channel-release problem is to **divide** a connection between A and B into a **sequence** of time ...
Cited by 248 - Related articles - View as HTML - All 10 versions

Toward an analytical approach to anonymous wireless networking [PDF] from psu.edu
P Venkitasubramaniam, T He... - Communications ..., 2008 - ieeexplore.ieee.org
... **Mix** is liable to be compro- mised, and hence a (possibly random) **sequence** of Mixes are ... Parallel to cryptography, secrecy in communi- cation has been studied extensively from an information theoretic ... Specifically, depend- ing on the routes in each session, we **divide** the set of ...
Cited by 2 - Related articles - BL Direct - All 5 versions

[BOOK] The design of Rijndael: AES--the advanced **encryption** standard
J Daemen ... - 2002 - books.google.com
... The new **encryption** standard was to become a Federal Information **Processing** Standard (FIPS). replacing the old Data **Encryption** Standard (DES) and triple-DES. Unlike the selection **process** for the DES. ... Page 22. 2 1. The Advanced **Encryption** Standard **Process** However. ...
Cited by 984 - Related articles - Library Search - All 5 versions

Regroup-And-Go mixes to counter the (< lT> n</lT>-1) attack
JQ Shi, BX Fang ... - Internet Research, 2006 - emeraldinsight.com
... Then, the total number of possible methods of **dividing** n messages into m groups with ... anonymous path, the sender's client program will randomly select a method to **divide** the messages ... injecting arbitrary messages, the RG **mix** can adopt the inter-**mix** link **encryption** scheme as ...
Related articles - BL Direct - All 4 versions

Create email alert